DETAILED ACTION

1. Supplemental Amendment filed 09/14/2010 has been received and considered.

2. Claims 1-43 are pending.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Bollman (Reg. No. 36457) on 09/28/2010.

The application has been amended as follows: Please replace claims 1, 10, 19, 28 and 36 as put forth below.

1. A method of processing out-of-order message packets, comprising:

obtaining a maximum largest nonce value;

comparing, with said secure communication module of said receiving client device, a nonce value of a received out-of-order message packet with a largest nonce value yet seen;

adjusting, with said secure communication module of said receiving client device, a size of a range of acceptable nonce values within a single replay attack acceptance window, where said size of said range is based on said largest nonce value yet seen;

comparing, with said secure communication module of said receiving client device, said largest nonce value yet seen with said maximum largest nonce value; and

resetting said largest nonce value yet seen and generating a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value.

10. An apparatus for processing out-of-order message packets, said apparatus comprising:

a receiving communication interface configured to transmit and receive a plurality of packets; and

a receiving controller, wherein said receiving controller is configured to:

obtain a maximum largest nonce value;

compare a nonce value of a received out-of-order message packet and a largest nonce value yet seen;

adjust a size of a range of acceptable nonce values within a single replay attack acceptance window, where said size of said range is based on said largest nonce value yet seen;

compare said largest nonce value yet seen with said maximum largest nonce value; and

resetting said largest yet seen and generating a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value.

19. A non-transitory computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of processing out-of- order message[[s]] packets, said one or more computer programs comprising a set of instructions for:

obtaining a maximum largest nonce value;

comparing, with said secure communication module of said receiving client device, a nonce value of a received out-of-order message packet and a largest nonce value yet seen;

adjusting, with said secure communication module of said receiving client device, a size of a range of acceptable nonce values within a single replay attack acceptance window, where said size of said range is based on said largest nonce value yet seen;

comparing, with said secure communication module of said receiving client device, said largest nonce value yet seen with said maximum largest nonce value; and

resetting said largest nonce value yet seen and generating a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value.

28. A system for processing out-of-order message packets in a peer-to-peer configuration, comprising:

a first peer configured to provide secure communication;

a second peer configured to provide said secure communication; and

a receiving secure communication module configured to be executed by said first peer and second peer, wherein said receiving secure communication module is configured to:

obtain a maximum largest nonce value;

compare a nonce value of a received out-of-order packet to a largest nonce value yet seen;

adjust a size of a range of acceptable nonce values within a single replay attack mask, where said size of said range is based on said largest nonce value yet seen;

compare said largest nonce value yet seen with said maximum largest nonce value; and

reset said largest nonce value yet seen and generate a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value.

36. A receiving interceptor device for processing out-of-order message packets, said receiving interceptor device comprising:

a network interface;

an expected sequence register configured to enumerate an expected sequence number of a message packet received out-of-order from a second network device; and

a receiving controller, wherein said receiving controller is configured to:

obtain a maximum largest nonce value;

compare a nonce value to of a received out-of-order message packet with a largest nonce value yet seen;

adjust a size of a range of acceptable nonce values within a single replay attack mask, where said size of said range is based on said largest nonce value yet seen;

compare said largest nonce value yet seen with said maximum largest nonce value; and

reset said largest nonce value yet seen and generate a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value.

Allowable Subject Matter

4. Claims 1-43 are allowed.

5. The following is an examiner's statement of reasons for allowance: The prior art generally teaches adjusting replay windows based on largest nonce values seen. However, the prior art fails to explicitly teach adjusting the size of the window based on the largest nonce value seen in combination with comparing the largest nonce value yet seen with a maximum largest nonce value and resetting the largest nonce value yet seen and generating a new cryptographic key when the largest nonce value exceeds the maximum largest nonce value.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Wong teaches the general concept of resetting a sliding window and Chapman teaches adjusting the size of a sliding window.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437